Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
Salena J. Chowdhury*
MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com
schowdhury@masonllp.com

David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada
Tel: (775) 329-1766
Tel: (703) 934-6377
dwise@wiselaw.pro

**pro hac vice forthcoming*

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

CAMILLE DAVIS, individually and on behalf of all others similarly situated, Plaintiff, v. PERRY JOHNSON & ASSOCIATES, INC., Defendant.	**Case No.** **CLASS ACTION** **COMPLAINT** **[JURY TRIAL DEMANDED]**

Plaintiff Camille Davis ("Plaintiff") brings this action on behalf of themselves and all others similarly situated against Defendant Perry Johnson & Associates, Inc. ("PJ&A" or "Defendant"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from PJ&A. Plaintiff(s) makes the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Perry Johnson & Associates, Inc.'s failure to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff's and Class Members' sensitive personal identifiable information that it acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack in May 2023 to compromise Defendant's network (the "Data Breach") that contained personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiff and other individuals ("the Class").

3. This class action arises out of a 2023 data breach ("Data Breach") of documents and information stored on the computer network of PJ&A, an online platform for medical transcribing services.

4. Accordingly, PJ&A notified the Department of Health and Human Services Office for Civil Rights ("HHS") on November 3, 2023, that this Data Breach included the Private Information of approximately 8,952,212 individuals, including Plaintiff and Class.[1]

5. In its Notice Letters, Defendant confirms that it "became aware of a

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 15, 2023).

potential data security incident impacting [its] systems" on May 2, 2023, and that third party may have copied and exfiltrated certain files containing Plaintiff's and Class Members' Private Information, including Social Security numbers.

6. Despite learning of the Data Breach on or about May 2, 2023 and determining that Private Information was involved in the breach, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until late October or early November 2023.[2]

7. As a result of PJ&A's Data Breach, Plaintiff and thousands of Class Members suffered ascertainable losses in the form of financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. In addition, Plaintiff's and Class Members' highly sensitive personal information—which was entrusted to Defendant—who claims that it "is committed to maintaining the privacy and security of the information [it] maintains."—was compromised and unlawfully accessed and extracted during the Data Breach.

9. Based upon PJ&A's notice letters, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-criminals who perpetrated this attack and remains in the hands of those cybercriminals.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information.

11. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been

[2] *See* https://www.pjats.com/downloads/Notice.pdf; and Website Notice Letter, Exhibit A.

subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

12. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. Defendant disregarded the privacy and property rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate and complete notice of the Data Breach.

14. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the intrusion sooner, notified Plaintiff and Class as well as the Attorneys General sooner, and potentially been able to mitigate the injuries to Plaintiff and the Class. According to its website notice letter, the "unauthorized party gained access to the PJ&A network between March 27, 2023, and May 2, 2023, and, during that time, acquired copies of certain files from PJ&A systems."[3]

15. Plaintiff's and Class Members' identities are now at substantial and

[3] https://www.pjats.com/downloads/Notice.pdf.

imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

16. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

17. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

18. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

20. Accordingly, Plaintiff brings this action against Defendant for negligence, negligence per se, breach of express contract, breach of implied contract, invasion of privacy, unjust enrichment, and declaratory relief, seeking redress for PJ&A's unlawful conduct.

21. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including

improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

22. 22. Plaintiff Camille Davis is and at all times relevant to this Complaint an individual citizen of the State of New York, residing in the city of Brooklyn. Plaintiff Davis was a patient of a PJ&A customer who received medical transcription services through PJ&A.

23. Perry Johnson & Associates, Inc. is a Nevada registered domestic corporation, which is headquartered in Henderson, Nevada. PJ&A's principal place of business is located at 1489 W. Warm Springs, Suite 110, Henderson, Nevada 89012. Defendant can be served through its registered agent at: C T Corporation System, 701 S Carson St. Ste 200, Carson City, Nevada 89701.

24. Plaintiff(s) reserves the right to seek leave to add other necessary defendants responsible for Plaintiffs' and Class Members' damages and injuries, including but not limited to any parent company, principals, manager, member, or affiliate of Perry Johnson & Associates, Inc.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

26. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a domestic corporation; it maintains its headquarters and principal place of

business in Nevada; and committed tortious acts in Nevada.

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which PJ&A has the most significant contacts.

STATEMENT OF FACTS

Nature of Defendant's Business.

28. PJ&A is a third-party service provider that provides medical transcription and reporting services.

29. PJ&A claims to "partners with the organizations that we work with to develop IT Solutions that increase process efficiencies, power better decision making and cut costs between 25-60%."[4]

30. PJ&A claims its "exclusively designed, web-based document management platform, GEMS, offers robust transcription and reporting services for medical professionals that will streamline provider workloads and improve patient care."[5] PJ&A, in the regular course of its business, collects and maintains the PII and PHI of individuals on behalf of its customers as a requirement of its business practices.

31. PJ&A provides third-party IT services to companies like Northwell Health, Inc. ("Northwell") and Cook County Health ("CCH"), collecting customer/patient data in order to provide a clinical documentation system that the customers can utilize for patient care.

32. The customers of PJ&A provide it with their patients' PII/PHI, with the mutual understanding that this highly sensitive private information will be kept confidential and properly safeguarded from misuse and theft.

33. In the course of collecting Private Information from consumers, including Plaintiff and Class Members, PJ&A promised to provide confidentiality

[4] https://www.pjats.com/contact-us// (last accessed Nov. 14, 2023).
[5] https://www.pjats.com/transcription-reporting/ (last accessed Nov. 14, 2023).

and adequate security for Private Information in compliance with statutory privacy requirements applicable to its industry. PJ&A is aware of and had obligations created by FTCA, HIPAA, contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and the Class Members, as consumers, relied on the promises and duties of PJ&A's customers and PJ&A itself to keep their sensitive PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Consumers, in general, demand that businesses that require highly sensitive Private Information will provide security to safeguard their Private Information, especially when Social Security numbers and private health information are involved.

36. In the course of their dealings with medical practice customers, PJ&A collects the following types of Private Information of Plaintiff and Class Members:

- Name
- Gender
- Address
- Contact details
- Date of birth
- Social Security number
- Driver license number and/or federal identification number
- Health information, diagnostics, and medical conditions

37. PJ&A had a duty, and was fully aware of its duty, to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from unauthorized disclosure to third parties.

The Data Breach.

38. According to its Notice Letters, on May 2, 2023, PJ&A became aware of "data security incident, which may have affected the privacy and security of your protected health information." Months between the date they "became aware" and sent the notice letters, its investigation determined that an unauthorized actor accessed the PJ&A network and exfiltrated the data of nearly **9 million individuals**, including Social Security numbers.[6]

39. The letter specifies that an unauthorized actor accessed PJ&A's network sometime around May 2, 2023 and was able to extract certain data from the network.

40. PJ&A reported to certain State Attorneys General websites that the accessed PII breached included: names, addresses, dates of birth, Social Security numbers, protected health information, and other information.[7]

41. On its own website notice letter, PJ&A stated the breached data "may include some or all of the following: name, date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service. . . For some individuals, however, the impacted data may have also included Social Security numbers, insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers."[8]

42. However, Plaintiff's and Class Members' PII and PHI was in the hands of cybercriminals for around *6 months before they were notified* of PJ&A's Data Breach. Time is of the essence when trying to protect against identity theft after a

[6] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 15, 2023).
[7] *See* Tex. Att'y Gen., *Data Breach Notifications*, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.
[8] https://www.pjats.com/downloads/Notice.pdf.

data breach, so early notification is critical.

43. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from PJ&A that included the Private Information of Plaintiff and Class Members.

44. Upon information and belief, the Private Information stored on PJ&A's network was not encrypted.

45. Plaintiff(s)' Private Information was accessed and stolen in the Data Breach. Plaintiff(s) reasonably believes their stolen Private Information, including Social Security numbers, is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

46. As a result of the Data Breach, PJ&A now encourages Class Members to spend time monitoring their accounts to protect themselves. This advice is both a direct encouragement to Plaintiff and the Class to spend time on self-protection efforts and a tacit admission of the imminent risk of identity theft faced by Plaintiff and Class Members.

47. PJ&A had obligations created by contract, industry standards, HIPAA as amended by HITECH, the FTCA, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

48. PJ&A could have prevented this Data Breach by, among other things, properly encrypting the PII and PHI entrusted to it, and by otherwise protecting and monitoring its network, computer equipment, and computer files containing Private Information.

Defendant Acquires, Collects, and Stores Private Information.

49. PJ&A acquires, collects, and stores a massive amount of Private Information of the patients of its customers for whom it is providing transcription

services.

50. By obtaining, collecting, and using Plaintiff's and Class Members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

51. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, including but not limited to being sure their medical providers, like the customers of PJ&A, abide by the privacy policies of HIPAA.

52. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach Was a

Foreseeable Risk of which Defendant Was on Notice

53. It is well known that Private Information, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect such information, including PJ&A, are well aware of the risk of being targeted by cybercriminals.

54. Individuals place a high value not only on their Private Information, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

55. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods,

services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[9]

56. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

57. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

58. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[10]

59. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[11]

60. Additionally in 2021, there was a 15.1% increase in cyberattacks and

[9] *Victims of Identity Theft, 2018*, U.S. Dep't of Justice (Apr. 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Nov. 14, 2023).
[10] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Nov. 14, 2023).
[11] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Nov. 14, 2023).

data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[12]

61. In light of high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its computer network would be targeted by cybercriminals.

62. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

63. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [13] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of

[12] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Nov. 14, 2023).
[13] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Nov. 14, 2023).

illegal activity."[14]

64. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, PJ&A failed to take appropriate steps to protect the Private Information of Plaintiff and the proposed Class from being compromised.

Data Breaches Are Rampant in Healthcare.

65. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

66. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[19]

67. Healthcare organizations, and the vendors they use like PJ&A, are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[20]

68. The HIPAA Journal article goes on to explain that patient records, like those stolen from PJ&A, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on

[14] *Id.*

individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[21]

69. Data breaches such as the one experienced by Defendant PJ&A have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

70. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[22]

71. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[23]

72. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[24]

73. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant PJ&A.

Defendant Fails to Comply with Industry Standards.

74. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

75. Several best practices have been identified that a minimum should be

implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

76. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

77. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

78. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Defendant's Conduct Violates HIPAA.

79. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

80. Covered entities must implement safeguards to ensure the

confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

81. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

82. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, " . . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. § 164.40.

83. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

At All Relevant Times Defendant Had a Duty to Plaintiff and Class Members to Properly Secure Their Private Information

84. At all relevant times, PJ&A had a duty to Plaintiff and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members

when PJ&A became aware that their Private Information was compromised.

85. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information.

86. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

87. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id*.

88. The ramifications of Defendant's failure to keep consumers' Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

The Value of Personal Identifiable Information

89. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[17]

90. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[18]

91. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity

[17] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Nov. 14, 2023).

[18] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last accessed Nov. 14, 2023).

can cause a lot of problems.[19]

92. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

93. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

94. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[21]

95. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate,

[19] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Nov. 14, 2023).

[20] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Nov. 14, 2023).

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Nov. 14, 2023).

birthplace, and mother's maiden name.[22]

96. Given the nature of this Data Breach, it is foreseeable that the compromised Private Information can be used by hackers and cybercriminals in a variety of devastating ways. Cybercriminals who possess Class Members' Private Information can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

97. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

98. Moreover, PJ&A has failed offer any identity theft monitoring and identity theft protection because of the data breach. Its failure to do so is grossly inadequate when victims are likely to face many years of identity theft. Now victims are forced to put forth out of pocket expenses and more time to mitigate identity theft. Victims will be forced to spend a significant amount of time un-doing the damage after the fraudulent acts occur with no help from PJ&A who is responsible for the repercussions of the data breach to victims.

99. In other words, Defendant expects Plaintiff and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

100. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

101. The injuries to Plaintiff and Class Members were directly and

[22] *See* OFFICE OF MGMT. & BUDGET, OMB MEMO. M-07-16 n.1 (last accessed Nov. 14, 2023).

proximately caused by PJ&A's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

102. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

103. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[24] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

104. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[25]

---

[23] FTC, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Nov. 14, 2023).

[24] FTC, *Protecting Personal Information* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Nov. 14, 2023).

[25] FTC, *Data Breach Response: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed Nov. 14, 2023).

105. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[26]

106. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an

[26] *See* FTC, *Start With Security*, *supra* note 28.

attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

107. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

108. Because Class Members entrusted Defendant through its customers with their Private Information, Defendant had, and has, a duty to the Plaintiff and Class Members to keep their Private Information secure.

109. Plaintiff and the other Class Members reasonably expected that when

they provide Private Information to Defendant (or to PJ&A's customers), Defendant would safeguard their Private Information.

110. PJ&A was at all times fully aware of its obligation to protect the personal data of consumers, including Plaintiff and Members of the Class. PJ&A was also aware of the significant repercussions if it failed to do so.

111. PJ&A's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Concrete Injuries Are Caused by Defendant's Inadequate Security.

112. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

113. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. Plaintiff and other individuals whose PII was entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

114. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff(s) have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging

adequate credit monitoring and identity theft protection services.

115. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

116. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

117. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

118. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

119. Accordingly, Defendant's wrongful actions and/or inaction and the

resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[27] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

120. As a result of the Data Breach, Plaintiff and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

121. PJ&A admits that an unauthorized third party accessed its servers on its computer systems. In other words, cybercriminals actually exfiltrated the PII that was accessed.[28]

Data Breaches Put Consumers at an Increased Risk
Of Fraud and Identify Theft

122. Data Breaches such as the one experienced Plaintiff and the Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

123. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[29] Its appendix

[27] *The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas*, https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed Nov. 14, 2023).
[28] *See* Website Notice Letter, Ex. A.
[29] https://www.gao.gov/assets/gao-19-230.pdf (last accessed Nov. 14, 2023), attached as Ex. B.

of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and the Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

124. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[30]

125. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

126. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[32]

127. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

---

[30] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Gov't Accountability Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 14, 2023) ("2007 GAO Report").

[31] *See* https://www.identitytheft.gov/Steps (last accessed Nov 14, 2023).

[32] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

128. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

129. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

Plaintiff Davis's Experience

130. Plaintiff Camille Davis is, and at all times relevant to this complaint, a resident and citizen of the State of New York.

131. Plaintiff Davis is an individual who was a patient at Northwell Health, Inc. which was a customer of PJ&A. To offer its medical transcription services, PJ&A required that the customer and/or Plaintiff Davis provide it with her Private Information, promising to guard her privacy.

132. Plaintiff is uncertain exactly what parts of her Private Information PJ&A has collected and stored. However, Plaintiff is aware that PJ&A collected PII/PHI from Northwell Health Inc.

133. PJ&A was entrusted with, collected, and stored Plaintiff's Private Information, including but not limited to her HIPAA protected medical information and Social Security number, from these various sources with the understanding that it had a duty to keep this Private Information safe and secure.

134. Around or after November 3, 2023, Plaintiff Bialka received the Notice of Data Breach letter, which indicated that PJ&A had known about the Data Breach for 5-6 months. The letter informed her that her critical Private Information was accessed by an unauthorized actor. The letter stated that the extracted information included her "name, date of birth, address, medical record number, account number, hospital account number, clinical information" and expanded on a long laundry list of other information that was also stolen. See Ex. A. She is not certain whether this list is exhaustive of all of her information that was stolen in PJ&A's data breach.

135. Plaintiff Davis is alarmed by the amount of her Personal Information that was stolen or accessed, and even more by the vast amount of highly personal information that was in the hands of PJ&A at the time of the breach on its computer system. See Ex. A.

136. Since PJ&A's data breach, Plaintiff Davis has been receiving an excessive amount of spam which she believes is directly related to her Private Information being stolen. Not only does this spam invade her privacy, dealing with it expends her time.

137. In response to PJ&A's Notice of Data Breach, Plaintiff is required to spend time dealing with the consequences of the Data Breach, which will continue. She has spent approximately 2 hours per week monitoring her accounts and expects that she will have to continue to do the same into the foreseeable future monitoring her credit and financial accounts as well as medical records and billing. PJ&A specifically advised Plaintiff to spend her time in these ways in its Notice Letter.

138. In addition, immediately after receiving the Notice Letter, Plaintiff

spent time verifying the legitimacy of the Notice of Data Breach, and considering credit monitoring and identity theft insurance options, and discussing her options with a law firm.

139. Plaintiff is very careful about sharing Private Information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She currently spends $29 per month on credit monitoring and has been notified that her Private Information has been found on the Dark Web.

140. Plaintiff suffered actual injury and damages as a result of the Data Breach in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to PJ&A directly or through her healthcare provider (the PJ&A customer).

141. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

142. Plaintiff Davis reasonably believes that her Private Information may have already been sold by cybercriminals.

143. Plaintiff Davis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, being placed in the hands of unauthorized third parties and possibly criminals.

144. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief remains backed up and in PJ&A's possession, is protected and safeguarded from future breaches. She remains at imminent risk of another Data Breach so long as PJ&A's computer networks are vulnerable to attack and her PII is not encrypted.

CLASS ACTION ALLEGATIONS

145. Plaintiff brings this action on behalf of themselves and on behalf of all

other persons similarly situated ("the Class").

146. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals whose Private Information was maintained on Perry Johnson & Associates, Inc.'s computer systems and who were sent a notice related the May 2023 Data Breach.

147. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

148. Plaintiff(s) hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

149. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff(s) at this time, based on information and belief, the Class consists of **nearly 9 million individuals** whose data was compromised in Data Breach.

150. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

A. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

B. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

C. Whether Defendant's data security systems prior to and during the

Data Breach complied with applicable data security laws and regulations;

D. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

E. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

F. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

G. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

H. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

I. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

J. Whether Defendant's conduct was negligent;

K. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

L. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

151. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

152. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel are competent and experienced in litigating class actions.

153. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members'

Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

154. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

155. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

156. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- Whether Defendant's security measures to protect its data

systems were reasonable in light of best practices recommended by data security experts;

- Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

157. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses, if not directly then through its customers, who were affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by PJ&A and its customers.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff and All Class Members)

158. Plaintiff(s) re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

159. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of the regular course of its business operations. Plaintiff and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

160. By collecting and storing Private Information in its computer property and using it for commercial gain, Defendant assumed a duty of care to use reasonable

means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could prevent and detect a breach of their security systems and to give prompt notice to those affected in the case of a Data Breach.

161. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

162. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

163. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

164. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

165. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

166. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

167. Defendant breached its duties to Plaintiff and Class Members under the

FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

168. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

169. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

170. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and Class Members had no ability to protect their Private Information that was in Defendant's possession.

171. Defendant was in a special relationship with Plaintiff and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiff and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiff's and Class Members' Private Information. The harm to Plaintiff and Class Members from its exposure was highly foreseeable to Defendant.

172. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

173. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See Restatement (Second) of Torts* § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

174. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

175. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

176. Defendant breached its duties of care by failing to adequately protect

Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiff and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

177. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

178. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

179. Through Defendant's acts and omissions described herein, including

but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

180. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

181. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

182. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

183. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

184. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT
Negligence Per Se
(On Behalf of Plaintiff and All Class Members)

185. Plaintiff(s) re-alleges and incorporates by the paragraphs above as if fully set forth herein.

186. Defendant's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

187. Defendant's duties also arise from, inter alia, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

188. Defendant violated Section 5 of the FTCA and HIPAA Privacy and Security Rules by failing to use reasonable measures to protect Plaintiff(s)' and other Class Members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

189. Defendant's violation of Section 5 of the FTCA and HIPAA Privacy and Security Rules constitutes negligence per se.

190. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA and HIPAA Privacy and Security Rules were intended to protect.

191. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA and HIPAA Privacy and Security Rules were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class Members as a result of the Data Breach.

192. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members'

PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII/PHI to unauthorized individuals.

193. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA and HIPAA Privacy and Security Rules. Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

THIRD COUNT
Breach of Express Contract
(On Behalf of Plaintiff and All Class Members)

194. Plaintiff(s) re-alleges and incorporates by the paragraphs above as if fully set forth herein.

195. Plaintiff and Class Members allege that they were the express, foreseeable, and intended third-party beneficiaries of valid and enforceable express contracts between Defendant and its customers (medical practices and hospitals that provided treatment to Plaintiff and Class Members), contracts that (upon information and belief) include obligations to keep sensitive Private Information private and

secure and inaccessible to unauthorized and criminal third-parties.

196. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (as patients of customers entering into the contracts).

197. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

198. The contract was therefore made primarily for the benefit of Plaintiff and Class Members, with Defendant promising to maintain the security of Plaintiff's and Class Members' PII while the Clients used Defendant's services to benefit Plaintiff and Class Members.

199. Defendant materially breached its contractual obligation to protect the Private Information of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

200. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

201. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their Private Information, the present risk of suffering additional damages, and out-of-pocket expenses including lost time spent monitoring and mitigating damages as Plaintiff and the Class were directly instructed to do by Defendant.

202. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

FOURTH COUNT

Invasion of Privacy
(On Behalf of Plaintiff and All Class Members)

203. Plaintiff(s) re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

204. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

205. Defendant owed a duty to individuals for whom it stored Private Information, including Plaintiff and the Class, to keep their PII and PHI confidential.

206. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII/PHI is highly offensive to a reasonable person.

207. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their PII/PHI both to their medical providers who retained Defendant's transcription services, but they did so with the intention that their information would be kept confidential and protected from unauthorized disclosure as Defendant promised in its Privacy Policy.

208. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

209. The Data Breach constitutes an intentional interference with Plaintiff(s)' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

210. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

211. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially

impairing their mitigation efforts.

212. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

213. As a proximate result of Defendant's acts and omissions, the PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

214. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their PII/PHI are still maintained by Defendant and its inadequate cybersecurity system and policies.

215. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential medical records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

216. In addition to injunctive relief, Plaintiff(s), on behalf of themselves and the other Members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FIFTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

217. Plaintiff(s) re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

218. This count is pled in the alternative to Plaintiff(s)' breach of contract claims above.

219. Plaintiff and Class Members conferred a monetary benefit on

Defendant in the form of the provision of their Private Information, and Defendant would be unable to engage in its regular course of business without their Private Information.

220. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

221. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

222. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

223. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

224. If Plaintiff and Class Members knew that Defendant had not sufficiently secured their Private Information, they would not have agreed to provide their Private Information directly or indirectly to Defendant.

225. Plaintiff and Class Members have no adequate remedy at law.

226. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

227. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

228. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from the collection and use of their Private Information for business purposes.

SIXTH COUNT
Declaratory Judgment
(On Behalf of Plaintiff and All Class Members)

229. Plaintiff(s) re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

230. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this

Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as alleged here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

231. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information.

232. Plaintiff(s) alleges that Defendant's data security measures remain inadequate. Plaintiff(s) will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

233. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. PJ&A continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes;

b. PJ&A continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

234. The Court also should issue corresponding prospective injunctive relief requiring PJ&A to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

235. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at PJ&A. The risk of another such breach is real, immediate, and substantial.

If another breach at PJ&A occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

236. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to PJ&A if an injunction is issued. Among other things, if another massive data breach occurs at PJ&A, Plaintiff and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to PJ&A of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and PJ&A has a pre-existing legal obligation to employ such measures.

237. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at PJ&A, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate

methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, and statutory damages, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: November 21, 2023

Respectfully submitted,

/s/ David Hilton Wise

David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
Salena J. Chowdhury*
MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com
schowdhury@masonllp.com

Attorneys for Plaintiff and the proposed Class

**pro hac vice forthcoming*